

Woosun Song

Github: github.com/pr0cf5

Email: wireless@kaist.ac.kr

EDUCATION

- **Korea Institute of Science and Technology**
 - *B.S candidate in Electrical Engineering and Computer Science*
 - GPA Total: 3.92/4.3, EE Major: 4.01/4.3, CS Major: 3.80/4.3

Daejeon, Korea
March 2018 - Present

SKILLS

- **English Proficiency**
 - TOEFL: 110/120
 - GRE General Exam: VR 161, QR 169, W 4.0
- **Programming Languages**
 - Python, C/C++, Rust, Assembly, JavaScript, Scala

INTERESTS

- **Computer Systems Security**
 - Code Analysis, Exploit Development

PUBLICATIONS

- **HardsHeap: A Universal and Extensible Framework for Evaluating Secure Allocators**
 - Insu Yun, **Woosun Song**, Seunggi Min, and Taesoo Kim
 - Proceedings of the 28th ACM Conference on Computer and Communications Security (CCS 2021) Seoul, South Korea, November 2021

PROJECTS

- **A Beginner-Friendly Tutorial on Kernel Exploitation**
 - Detailed guidelines on environment setup: compiling Loadable Kernel Modules and running them via QEMU
 - Discusses popular techniques to bypass Linux Kernel exploit defenses such as SMEP/SMAP/kPTI.
 - Link: github.com/pr0cf5/kernel-exploit-practice
- **dTLB Timer: Measuring L1 dTLB Latency Under the Absence of Fine Grained Timing Primitives**
 - Term project for KAIST 2022 Spring EE595: Hardware Security
 - Intermediate work for constructing a Spectre-v1 PoC for web browsers
 - Proposed a method to reverse engineer the pLRU replacement policy of Intel Skylake's L1 dTLB
 - Contains a working PoC in JavaScript/WebAssembly that uses DOM's `performance.now()` API for time measurement
 - Link: github.com/pr0cf5/dtlb-timer

HONORS AND AWARDS

- **CTF(Capture-The-Flag) Competitions**
 - HXP CTF 2021, 2nd place (with team Super Guesser)
 - DEFCON CTF 27 Finals, 12th place (with team KaisHackGoN)
 - Codegate CTF 2019 University Division, 3rd place (with team GoN)
- **Academic Awards & Scholarships**
 - KAIST Freshman Dean's List, 2018 Spring
 - National Science & Technology Scholarship (2019 Fall - Present)

EXPERIENCE

- **CTF Challenge Author**
 - Cyber Operations Challenge 2020 qual (2 tasks)
 - Cyber Operations Challenge 2020 final (1 task)
 - Codegate CTF 2020 preliminary (2 tasks)
 - Codegate CTF 2020 final (1 task)
 - GoN Qual CTF 2022 (1 task)
 - WACon CTF 2022 (3 tasks)
 - **Mandatory Military Service**
 - Enlisted in Korea Army, English interpreter
- Busan, South Korea
Aug 2020 - Feb 2022